01_Linuxサーバデータベース - Ubuntu20.04のOpenSSLを1.1.1から3.1.1にアップデート。

概要

2023/09/11にサポート終了を迎えるOpenSSL1.1.1。

2023年6月現在の最新安定版である3.1.1にアップデートを行います。

https://www.openssl.org/blog/blog/2023/06/15/1.1.1-EOL-Reminder/

環境

- OS:Ubuntu 20.04

```
openssl version -a

OpenSSL 1.1.1f 31 Mar 2020
built on: Wed May 24 17:14:51 2023 UTC
platform: debian-amd64
options: bn(64,64) rc4(16x,int) des(int) blowfish(ptr)
compiler: gcc -fPIC -pthread -m64 -Wa,--noexecstack -Wall -Wa,--noexecstack -g -O2 -fdebug-prefix-map=/build/openssl-mSC
/openssl-1.1.1f=. -fstack-protector-strong -Wformat -Werror=format-security -DOPENSSL_TLS_SECURITY_LEVEL=2 -DOPENSSL_U
SE_NODELETE -DL_ENDIAN -DOPENSSL_PIC -DOPENSSL_CPUID_OBJ -DOPENSSL_IA32_SSE2 -DOPENSSL_BN_ASM_MONT -DOP
ENSSL_BN_ASM_MONT5 -DOPENSSL_BN_ASM_GF2m -DSHA1_ASM -DSHA256_ASM -DSHA512_ASM -DKECCAK1600_ASM -DR
C4_ASM -DMD5_ASM -DAESNI_ASM -DVPAES_ASM -DGHASH_ASM -DECP_NISTZ256_ASM -DX25519_ASM -DPOLY1305_ASM
-DNDEBUG -Wdate-time -D_FORTIFY_SOURCE=2
OPENSSLDIR: "/usr/lib/ssl"
ENGINESDIR: "/usr/lib/x86_64-linux-gnu/engines-1.1"
Seeding source: os-specific
```

参考とした手順

https://nextgentips.com/2022/03/23/how-to-install-openssl-3-on-ubuntu-20-04/

さっくりとした手順

1. システム全体のバックアップ
2. 必要なライブラリをインストールします。
3. githubレポジトリから最新安定版のソースコードをダウンロードします。
4. ソースからインストールしていきます。
5. 設定を行います。（コンフィグを反映させ、パスを通します）
6. バージョンアップを確認します。
7. 自動アップデートを無効化します。

実施した手順

全体のバックアップを取得します。

- Webアクセスの根幹となるプログラムであること
- 重要なデータが格納されている

ことから、AWS Lightsailのスナップショットを利用して全体のバックアップを取りました。

必要なライブラリのインストール

```
sudo aptitude install build-essential checkinstall zlib1g-dev git
#  筆者はaptitudeを用いています。必要に応じてaptを使ってください。
```

ソースコードの取得

```
sudo su -
#  以下、管理者権限で実施します

cd /hoge
#  任意のディレクトリを指定します
```

```
git clone https://github.com/openssl/openssl -b openssl-3.1.1
#  2023/06/20時点での最新安定版を指定します

cd openssl
```

ソースからインストール

```
./config --prefix=/usr/local/ssl --openssldir=/usr/local/ssl shared zlib

make
#  makeは時間がかかります。状況を時折確認しながら待ちましょう。

make test

make install
```

インストール後の設定

- 設定ファイル追記

```
cat <<- __EOF__ | tee -a /etc/ld.so.conf.d/openssl-3.1.1.conf
/usr/local/ssl/lib64
__EOF__
```

- 設定反映

```
ldconfig -v
```

- 既存プログラムの退避

```
mv /usr/bin/c_rehash /path/to/backup/c_reha$(date +%Y%m%d)l

mv /usr/bin/openssl /path/to/backup/opens$(date +%Y%m%d)l
#  任意の退避ディレクトリを指定します
```

- パスを通す

```
cat <<- __EOF__ | tee -a /etc/environment
PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/usr/local/ssl/bin"
__EOF__
```

- 通したパスを反映

```
source /etc/environment

echo $PATH
#  PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/usr/local/ssl/bin"
#  と表示されることを確認します
```

バージョンアップ後の確認

```
openssl version -a

OpenSSL 3.1.1 30 May 2(Library: OpenSSL 3.1.1 30 May ) 2023
built on: Tue Jun 20 01:47:24 2023 UTC
platform: linux-x86_64
options: (64,64)
compiler: gcc-fPIC -pthread -m64 -Wa,--noexecstack -Wall -O3 -DOPENSSL_USE_NODELETE -DL_ENDIAN -DOPENSSL_PIC
-DOPENSSL_BUILDING_OPENSSL -DZLIB -DNDEBUG
OPENSSLDIR: "/usr/local/ssl"
ENGINESDIR: "/usr/local/ssl/lib64/engines-3"
MODULESDIR: "/usr/local/ssl/lib64/ossl-modules"
Seeding source: os-specific
CPUINFO: OPENSSL_ia32cap=0x7ffaf3ffffebffff:0x27ab
```

これで、Ubuntu20.04でもOpenSSL3.1.1を利用することが可能になりました。

必要に応じて

- システムの再起動を行います。
- 既存サービスが正常に動くことを確認します。

自動アップグレード無効

強制的に3.1系に上げるので、その後、1.1.xがアップグレードされる可能性を防ぎます。

```
#  apt  を使用する場合
sudo  apt-mark  hold  openssl

#  aptitude  を使用する場合
sudo  aptitude  hold  openssl
```

ファイル

O_春節でパソコンを使うお姉さん2024010507(ftmm).jpg	225 KB	2024/01/05	手動人形